

REMARKS/ARGUMENTS

The Office Action has been carefully considered. The issues raised are traversed and addressed below with reference to the relevant headings and paragraph numbers appearing under the Detailed Action of the Office Action.

Specification

The amendment to the co-pending applications paragraph on Page 1 is merely to update the application numbers to patent numbers. We have also deleted application numbers for those cases which were inadvertently added but not filed until after the filing date of this application.

Claim Rejection – 35 USC § 103

In view of the Examiner's continued objections to the claims the claims have been substantially revised to further clarify the interactions performed between the printer and the registration server during the registration protocol.

In particular, the claim has been revised to clarify that the printer and registration server determine a session key. The claim then goes on to clarify that the printer transmits a message formed by encrypting the secret unique identifier, a public unique identifier and a public key of a public/private key pair. This is intended to clarify the nature of the "secure" transmission previously referred to in the claim and a basis for this can be found for example on page 50, lines 14 to 19, and in Figure 50.

The claim then goes on to clarify that the registration server authenticates the printer by decrypting the message using the session key and using the public identifier to obtain the secret unique identifier from the database again, as shown in Figure 50.

The registration server then compares the secret unique identifier installed in the database with the secret unique identifier received in the message to authenticate the printer, with the registration server generating and storing a certificate in the registration database if this authentication is successful. Again a basis for this can be found for example on page 50, line 30 to page 51, line 10.

In view of the amendments made to the claims, we respectfully submit that this clarifies the nature of the interaction and this defines a claim which is novel and inventive over the cited prior art.

In particular, during previous prosecution the Examiner has indicated that Debry describes providing a secret identifier and a public identifier. However, we respectfully submit that there is no discussion in Debry of providing both a secret unique identifier and a public unique identifier, both of which are encrypted in a message, together with a public key, using a session key.

The Examiner has referred to Newton as describing a unique identification key which is compared to a key stored in a server database and which is encrypted during transmission. However, this again does not describe encrypting both a secret unique identifier and a public unique identifier, with the public unique identifier being useable to obtain the secret unique identifier from the database.

In view of this, we do not believe that any of the cited documents describe using a message formed by encrypting, using a session key, a secret unique identifier, a public unique identifier and a public key of a public/private key pair.

We also note that the claim now requires that the registration server generate and store the certificate containing the printers public unique identifier and associated public key.

These features were previously included in claim 7 which the Examiner rejected on the basis of Debry. In this regard, the section of Debry referred to by the Examiner clearly states that the server build a digital certificate which is sent to the printer. This allows the printer to determine a public/private key pair from the certificate. The section goes on to specify that the certificate authority stores a public key associated with the device. Thus, this portion of Debry is very explicit in stating that the certificate is sent to the printer whilst the public key is stored in a database.

In contrast to this, the claim 1 now requires that the certificate is stored in the registration database. Furthermore, it is not necessary to transmit the certificate to the printer as the printer has already supplied the public key during the registration process and therefore does not need to determine the public/private key pair. We would therefore highlight that Debry does not describe transmitting a public key of a public/private key pair to the registration server which is then used to create the registration certificate.

In view of the amendments made to claim 1, claims 4, 5 and 7 have now been cancelled from the application. In addition to this a new claim 9 has been provided which relates to the printer per se. In addition to this, claim 10 and 11 have been added which refer to the printer generating the public/private key pair which is not disclosed in Debry as discussed above and with the printer communicating with the server using the defined method, a basis for which can be found on page 51 as previously mentioned. Finally, a new claim 12 has been added which clarifies that the printer acts as a relay device to allow a sensing device to communicate via the network.

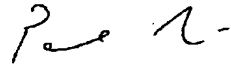
CONCLUSION

In light of the above, it is respectfully submitted that the objections and claim rejections have been successfully traversed and addressed. The amendments do not involve adding any information that was not already disclosed in the specification, and therefore no new matter is added.

Accordingly, it is respectfully submitted that the claims, and the application as a whole with these claims, are allowable, and a favourable reconsideration is therefore earnestly solicited.

Very respectfully,

Applicant:



PAUL LAPSTUN



KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762